

WHAT IS CLAIMED IS:

1 1. A security management apparatus comprising:

2 a security diagnostic unit for making a security diagnosis on a basis of
3 security information obtained from a security information providing unit for
4 providing information concerning security in a network and further on a basis of
5 machine information obtained from at least one network machine connected to
6 a network to judge a type of security-related processing to be executed for said
7 network machine or a predetermined network including said network machine
8 and also judge whether or not the security-related processing needs to be
9 executed; and

10 a security execution unit for executing predetermined security measure
11 processing for said network machine or the predetermined network including
12 said network machine on a basis of a result of diagnosis made by said security
13 diagnostic unit.

1 2. A security management apparatus according to claim 1, wherein
2 said security diagnostic unit further uses machine-related information obtained
3 from a machine-related information storage unit containing predetermined
4 information about network machines that are connected to said network or may
5 be connected to said network to judge a type of security-related processing to
6 be executed for said network machine or the predetermined network including
7 said network machine and also judge whether or not the security-related
8 processing needs to be executed.

1 3. A security management apparatus according to claim 2, wherein the
2 machine-related information stored in said machine-related information storage
3 unit is information specifying a security policy.

1 4. A security management apparatus according to claim 1, further
2 comprising:

3 a connection request accepting unit for accepting a connection request
4 from a newly introduced network machine;

5 wherein when said connection request accepting unit accepts a
6 connection request from a newly introduced network machine, said security
7 diagnostic unit assigns an address to said newly introduced network machine
8 after placing it in an isolated state and judges whether or not to execute
9 processing for unisolating said newly introduced network machine as said
10 security-related processing on a basis of said machine information and said
11 security information.

1 5. A security management apparatus according to claim 1, further
2 comprising:

3 a connection request accepting unit for accepting a connection request
4 from a newly introduced network machine;

5 wherein when said connection request accepting unit accepts a
6 connection request from a newly introduced network machine, said security
7 diagnostic unit receives machine information from said newly introduced
8 network machine and judges whether or not to execute processing for
9 assigning an address to said newly introduced network machine as said
10 security-related processing on a basis of said machine information and said
11 security information.

1 6. A security management apparatus comprising:

2 a security diagnostic unit for making a security diagnosis on a basis of
3 machine information obtained from at least one network machine connected to

4 a network and further on a basis of machine-related information obtained from
5 a machine-related information storage unit containing predetermined
6 information about network machines that are connected to said network or may
7 be connected to said network to judge a type of security-related processing to
8 be executed for said network machine or a predetermined network including
9 said network machine and also judge whether or not the security-related
10 processing needs to be executed; and

11 a security execution unit for executing predetermined security measure
12 processing for said network machine or the predetermined network including
13 said network machine on a basis of a result of diagnosis made by said security
14 diagnostic unit.

1 7. A security management apparatus according to claim 6, wherein
2 said machine-related information includes information indicating behavior of
3 computer viruses, and said machine information includes at least either one of
4 a hash value of a predetermined file and a virus scan result; and

5 said security diagnostic unit judges whether or not a predetermined
6 network machine needs to be isolated, and said security execution unit
7 executes processing for isolating said network machine when said security
8 diagnostic unit judges that said network machine needs to be isolated.

1 8. A security management apparatus according to claim 6, further
2 comprising:

3 a network monitor for monitoring communications on said network
4 machines;

5 wherein said machine-related information is information concerning a
6 network machine profile;

7 said security diagnostic unit judges whether or not a predetermined

8 network machine needs to be isolated on a basis of monitor information
9 obtained from said network monitor and said machine information and further
10 said network machine profile information; and

11 said security execution unit executes processing for isolating said
12 network machine when said security diagnostic unit judges that said network
13 machine needs to be isolated.

1 9. A security management apparatus according to claim 6, wherein
2 said security diagnostic unit identifies a range of damage and determines a
3 range of isolation.

1 10. A security management apparatus according to claim 6, further
2 comprising:

3 a recovery unit for repairing a network machine or network having
4 received predetermined damage on a basis of a result of diagnosis made by
5 said security diagnostic unit.

1 11. A security management apparatus according to claim 6, further
2 comprising:

3 an unisolating unit for canceling isolation when damage repair has
4 been made.

1 12. A security management apparatus according to claim 6, wherein
2 said machine information includes a notice of a change in equipment
3 configuration and at least information concerning the equipment configuration
4 that may be changed, and said machine-related information includes
5 equipment configuration information specifying whether or not the network
6 machine is usable in said network.

1 13. A security management system comprising:

2 a security information providing apparatus for providing security
3 information concerning security in a network;

4 a machine-related information database containing predetermined
5 information about network machines that are connected to said network or may
6 be connected to said network;

7 a preventive system for judging whether or not there is damage to at
8 least one network machine connected to a network or damage to a
9 predetermined network including said network machine or whether or not
10 preventive measures need to be executed for said network machine or said
11 predetermined network on a basis of security information obtained from said
12 security information providing apparatus and machine-related information
13 obtained from said machine-related information database and further machine
14 information obtained from said network machine; and

15 a recovery system for executing recovery processing when there is
16 predetermined damage, or taking preventive measures on a basis of judgment
17 made by said preventive system.

1 14. A security management system according to claim 13, wherein a
2 plurality of said preventive systems or a plurality of said recovery systems are
3 provided, and a management center for generally managing these systems is
4 provided.

1 15. A security management system according to claim 13, wherein
2 said preventive system and said recovery system are provided on a side of an
3 owner of said security information providing apparatus.

1 16. A security management system according to claim 13, wherein

2 said preventive system is provided on a side of an owner of said security
3 information providing apparatus, and said recovery system is provided on a
4 side of a management service provider who provides management services.

1 17. A security management system according to claim 13, wherein
2 said preventive system and said recovery system are provided on a side of a
3 management service provider who provides management services.

1 18. A security management system according to claim 13, wherein
2 predetermined information obtained by said recovery system is fed back to
3 said preventive system as new security information.

1 19. A security management method comprising the steps of:
2 obtaining security information concerning security in a network;
3 obtaining machine information from at least one network machine
4 connected to a network;
5 making a security diagnosis on a basis of said security information and
6 said machine information to judge a type of security-related processing to be
7 executed for said network machine or a predetermined network including said
8 network machine and also judge whether or not the security-related processing
9 needs to be executed; and
10 executing predetermined security measure processing for said network
11 machine or the predetermined network including said network machine on a
12 basis of a result of diagnosis made by said security diagnostic step.

1 20. A security management method according to claim 19, further
2 comprising the step of obtaining machine-related information from a machine-
3 related information storage unit containing predetermined information about

4 network machines that are connected to said network or may be connected to
5 said network;

6 wherein said security diagnostic step makes said security diagnosis on
7 a basis of said machine-related information as well as said security information
8 and said machine information.

1 21. A security management method comprising the steps of:

2 obtaining machine information from at least one network machine
3 connected to a network;

4 obtaining machine-related information from a machine-related
5 information storage unit containing predetermined information about network
6 machines that are connected to said network or may be connected to said
7 network;

8 making a security diagnosis on a basis of said machine information
9 and said machine-related information to judge a type of security-related
10 processing to be executed for said network machine or a predetermined
11 network including said network machine and also judge whether or not the
12 security-related processing needs to be executed; and

13 executing predetermined security measure processing for said network
14 machine or the predetermined network including said network machine on a
15 basis of a result of diagnosis made by said security diagnostic step.

1 22. A security management program for instructing a computer to
2 execute security management, said program comprising the steps of:

3 obtaining security information concerning security in a network;

4 obtaining machine information from at least one network machine
5 connected to a network;

6 making a security diagnosis on a basis of said security information and

7 said machine information to judge a type of security-related processing to be
8 executed for said network machine or a predetermined network including said
9 network machine and also judge whether or not the security-related processing
10 needs to be executed; and

11 executing predetermined security measure processing for said network
12 machine or the predetermined network including said network machine on a
13 basis of a result of diagnosis made by said security diagnostic step.

1 23. A security management program according to claim 22, further
2 comprising the step of obtaining machine-related information from a machine-
3 related information storage unit containing predetermined information about
4 network machines that are connected to said network or may be connected to
5 said network;

6 wherein said security diagnostic step makes said security diagnosis on
7 a basis of said security information and said machine information and further
8 said machine-related information.

1 24. A security management program for instructing a computer to
2 execute security management, said program comprising the steps of:

3 obtaining machine information from at least one network machine
4 connected to a network;

5 obtaining machine-related information from a machine-related
6 information storage unit containing predetermined information about network
7 machines that are connected to said network or may be connected to said
8 network;

9 making a security diagnosis on a basis of said machine information
10 and said machine-related information to judge a type of security-related
11 processing to be executed for said network machine or a predetermined

12 network including said network machine and also judge whether or not the
13 security-related processing needs to be executed; and
14 executing predetermined security measure processing for said network
15 machine or the predetermined network including said network machine on a
16 basis of a result of diagnosis made by said security diagnostic step.